FKCC
SUBJECT: Enclosure to US Forces Korea (USFK) Command Policy Letter # 5, Operations Security (OPSEC)

USFK OPSEC Protective Measures

The following OPSEC measures should be integrated in daily operations by all USFK personnel. Through vigilance in these seven areas, we can mitigate or reduce many disclosures of sensitive information and operational indicators. Based on unique mission requirements and activities, additional measures will likely be needed to fully protect command and unit critical information.

1. Computer Network Activities:

a. Use the appropriate secure network (i.e., CENTRIXS-K, SIPRNET) anytime you process classified information. This is also the preferred method when working on or transmitting sensitive unclassified information.

b. As a minimum, encrypt NIPRNET email using your Common Access Card (CAC) every time you pass sensitive unclassified information and unit Critical Information. This information should ***never*** be transmitted using commercial internet service providers, period.

c. To protect sensitive unclassified and potentially classified information, properly label and control removable computer media (i.e., CD/DVD, disk, removable hard drive, etc).

2. Telephone and Radio Communications:

a. Use a secure telephone (STE or VoIP) or encrypted radio for passing sensitive information.

b. Do not attempt to "talk around" classified or sensitive information on an open line.

c. Announce "phone up/down" and use push-to-talk handsets properly.

d. If cellular phones are authorized in the facility, deactivate them (remove the battery) prior to entering a classified working area, command post/operations center, or where classified or sensitive discussions may take place.

3. Public Information Releases:

a. Get approval from your chain of command before talking with any media representative. Refer all requests for information to the Public Affairs Office.

b. Do not post sensitive operational information or information that could be used to target friendly forces or family members to official publicly accessible or personal websites, weblogs, or chat rooms.

c. Keep sensitive discussions in the workplace.

4. Social Networking Sites:

a. Assess the risk before posting information about you or your organization. Never post sensitive or critical information. Post information as if privacy or filtering settings do not exist within the site's functionality.

b. Set privacy settings to protect personal information and control how much is revealed about you and to whom.

c. Before accepting a friend/connection request, directly confirm the request with them. This ensures that the involved accounts are neither compromised nor impersonated.

d. Be selective about which third-party applications to add to your profile. These applications could contain malicious code that can compromise your computer or your organization's network.

e. Follow computer security guidelines. Do not use official email addresses on these sites and secure your password.

5. Document Disposal: Shredded papers are of no use to our adversaries. Shred ALL documents or paper that are work-related or contain personal information.

6.. Know Command Critical Information: Know what to protect; post the command/unit Critical Information List at all desks and workstations where information is processed and transmitted.

7.. Immediately report all suspicious activities, persons, and objects.